

(19)



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11)

EP 0 951 155 A1

(12)

## DEMANDE DE BREVET EUROPEEN

(43) Date de publication:  
20.10.1999 Bulletin 1999/42

(51) Int Cl. 6: H04L 12/24

(21) Numéro de dépôt: 99400808.4

(22) Date de dépôt: 02.04.1999

(84) Etats contractants désignés:  
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE  
Etats d'extension désignés:  
AL LT LV MK RO SI

(30) Priorité: 15.04.1998 FR 9804695

(71) Demandeur: BULL S.A.  
78430 Louveciennes (FR)

(72) Inventeurs:  
• Brunet, Jean  
35830 Betton (FR)  
• Lamberet, Florence  
78170 La Celle Saint Cloud (FR)

(74) Mandataire: Denis, Hervé et al  
Direction de la  
Propriété Industrielle Bull S.A.  
Poste courrier: LV-58F35  
68, route de Versailles  
78434 Louveciennes Cedex (FR)

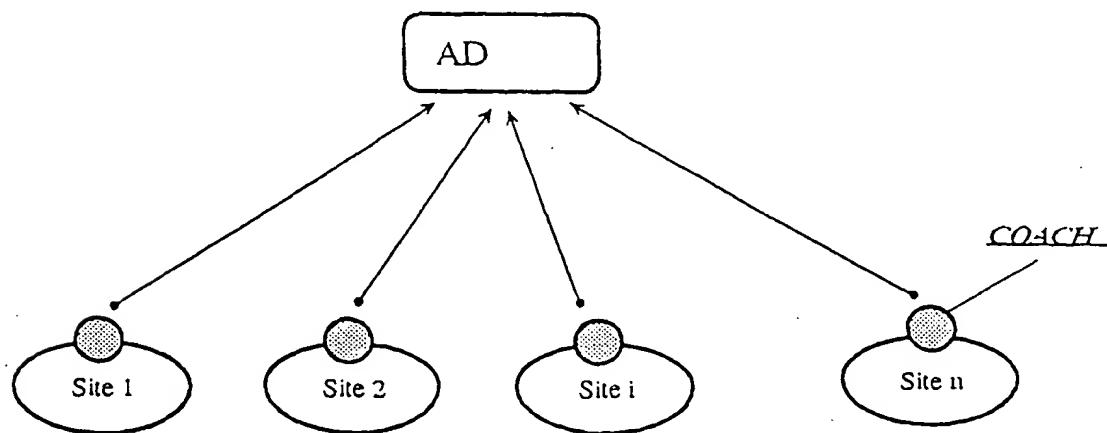
### (54) Procédé et système d'administration de réseaux et de systèmes

(57) La présente invention concerne un procédé et un système d'administration de réseaux et de systèmes.

Le procédé d'administration d'un réseau est caractérisé en ce qu'il comprend au moins un sous-administrateur (COACH) situé dans l'arbre de contenance entre un administrateur principal (AD) et les équipements du réseau, le sous-administrateur étant localisé sur le ré-

seau local d'entreprise (RLE), administrant un sous-réseau et comprenant différents modules qui communiquent entre eux et avec un administrateur principal (AD) par l'intermédiaire d'un noyau (N), les modules interrogeant les équipements du sous-réseau et recevant les alarmes lancées par les agents (snmp) fonctionnant sur les équipements du sous-réseau.

### FIG. 3



**Description**

[0001] La présente invention concerne un procédé et un système d'administration de réseau et de systèmes.

[0002] Les grandes entreprises ont un nombre croissant d'équipements à gérer. Ces équipements, reliés entre eux par un réseau de communication appelé "Réseau Local d'Entreprise" (RLE, LAN), sont administrés par un administrateur. Pour administrer (contrôler, agir, surveiller, piloter) à distance des équipements à partir d'un point, le modèle d'architecture comportant un administrateur, par exemple, (ISM, figure 4) et un agent, par exemple, type SNMP, est le plus couramment adopté. Dans ce modèle d'architecture, les agents (SNMP), implantés sur les équipements (ET) du réseau, renseignent l'administrateur sur l'état de chacun des équipements administrés. Lors de chaque dysfonctionnement d'un équipement, un agent (snmp) envoie, à l'administrateur, une alarme à travers le réseau grande distance (WAN). Dans la grande majorité des cas, cet administrateur gère plusieurs centaines d'équipements répartis sur un ou plusieurs pays. Les informations échangées entre l'administrateur et les équipements administrés circulent à travers un réseau grande distance aussi appelé "WAN" (Wide Area Network). Cependant, le réseau WAN a des capacités limitées et la transmission des informations à travers ce réseau est aujourd'hui lente et peu sûre. Ce problème s'explique par le fait que la bande passante du réseau (WAN) est trop réduite par rapport au nombre d'informations toujours croissant devant transiter entre les administrateurs et leurs équipements. Les réseaux locaux supportent souvent un trafic supérieur à 10 Mégabits, alors que le réseau WAN a une largeur de bande souvent inférieure ou égale à 64 Kilobits : 9600 bauds est une valeur courante. En conséquence, le réseau (WAN) est saturé et beaucoup d'informations sont perdues. D'autre part, la transmission des données est très lente et le type d'envoi (par petits paquets périodiques) n'est pas adapté aux modes courants d'utilisation des WANS. Le traitement des informations par l'administrateur est ralenti et les actions correctrices à déclencher sont tardives. De plus, dans certains cas, la chronologie des arrivées des informations à l'administrateur n'est pas respectée à cause de ce flux trop important. Dans ce cas, le traitement de ces informations peut donner lieu à une mauvaise interprétation des faits qui peut déclencher des actions inadéquates de la part de l'administrateur. Le coût des communications est, par ailleurs, élevé.

[0003] Une solution au problème de perte d'informations consiste en ce que l'administrateur génère à travers le réseau (WAN), à une période donnée, une requête de la forme "Est-ce que tu vas bien ?" vers chaque système administré et que ces derniers répondent "Oui, je vais bien". Cette solution est très coûteuse. Elle ne résout pas le problème de sursaturation des câbles et augmente encore les flux d'informations à travers le réseau (WAN). En outre, la requête ou la réponse à cette requête peut se perdre dans le réseau (WAN).

[0004] Une autre solution consiste à gérer les flux d'informations à l'aide d'outil tel que SM Monitor 6000 proposé par la marque IBM. Cet outil, fortement lié à la plate-forme appelée "System View", est déporté et permet de concentrer les alertes d'un réseau et d'effectuer des opérations à partir des informations que peuvent fournir les agents du réseau. Mais, SM Monitor 6000 est consommateur d'unité centrale de traitement (CPU, Control Processing Unit) et prend une place importante en mémoire. De plus, aujourd'hui, un grand nombre d'entreprises a besoin de gérer des petits réseaux en grand nombre. Or, SM Monitor 6000 ne possède pas de mécanisme de déploiement à grande échelle et ne peut donc pas être utilisé pour la gestion d'un grand nombre d'équipements. En outre, SM Monitor 6000 a une technologie peu portable. La configuration de SM Monitor 6000 ne peut s'effectuer qu'avec la plate-forme "System View" et est inexploitable sans cet outil.

[0005] Une dernière solution, proposée par la société "BMC software", consiste en un module de contrôle qui permet de surveiller un ensemble d'agents appelés "agents Patrols". Un agent Patrol peut contenir plusieurs modules, chacun ayant pour fonction de récolter un certain type d'informations tel que les informations du système ou les informations d'une application (par exemple, d'une base de données Oracle). Cette solution n'est pas adaptée. En effet, bien que la technologie Patrol permette de récolter certaines informations sur les équipements, elle n'est pas conçue pour assurer un rôle d'administrateur vis-à-vis d'agents. L'agent Patrol traite des données locales sur une machine, il n'est qu'une source d'informations et ne s'alimente pas de données en provenance d'autres agents. En outre, la capacité à gérer le changement sur les équipements est ignorée par l'approche de Patrol, alors qu'elle est fondamentale en exploitation. De plus, elle est consommatrice de temps et moyens CPU des systèmes cibles à cause de la technologie par langage interprété.

[0006] La présente invention a pour but de pallier des inconvénients de l'art antérieur en proposant un procédé portable d'administration de réseaux adapté à l'administration d'un grand nombre d'équipements. Le procédé selon l'invention, limite et sécurise le flux d'administration entre l'administrateur et les équipements administrés en évitant l'envoi de messages non nécessaires ou la répétition de l'envoi d'un même message dans le réseau WAN. Ce procédé s'adapte ainsi, aux saturations de la bande passante et permet de réduire les pertes d'informations dans le réseau (WAN). De plus, grâce à ce procédé, les fréquences de récolte d'informations sont adaptables, information par information, et les données récoltées par le système sont réutilisables à tout moment pour effectuer des statistiques, pour surveiller les performances des équipements ou encore pour éviter d'aller rechercher plusieurs fois la même information. D'autre part, ce système s'auto-instruit de son environnement. La prise en compte de milliers d'équipements se fait automatiquement malgré des contextes très différents. L'apparition et la disparition de systèmes démontables sont

dynamiquement prises en compte au cours de l'exploitation, sans intervention de l'opérateur. Enfin, l'invention permet une diminution de la charge de traitements d'informations au niveau du contrôle.

[0007] Ce but est atteint par le fait que le procédé d'administration d'un réseau comprend au moins un sous-administrateur (COACH) situé dans l'arbre de contenance entre un administrateur principal (AD) et les équipements du réseau, le sous-administrateur est localisé sur le réseau local d'entreprise (RLE), administre un sous-réseau et comprend différents modules qui communiquent entre eux et avec un administrateur principal (AD) par l'intermédiaire d'un noyau (N), les modules interrogeant les équipements du sous-réseau et recevant les alarmes lancées par les agents (snmp) fonctionnant sur les équipements du sous-réseau, le procédé étant composé de plusieurs étapes :

- 10 - une étape pendant laquelle un module de découverte (MD) interroge tous les équipements (ET) possibles du sous-réseau.
- une étape de recherche de domaine par le module de découverte (MD), lorsqu'un équipement répond à l'interrogation (SNMP),
- une étape pendant laquelle le module de découverte (MD) envoie une notification à un module de configuration des modèles (MCM) lui indiquant l'adresse internet (IP) de l'équipement découvert et le domaine auquel l'équipement découvert appartient,
- une étape pendant laquelle le module de configuration des modèles (MCM) notifie à un module de calcul d'indicateurs (MCI), l'indicateur à instancier sur l'équipement et à un module de filtrage d'alarmes (MFA) le modèle de filtre à instancier sur l'équipement.

[0008] Selon une particularité de l'invention, le procédé d'administration d'un réseau est caractérisé en ce qu'à chaque nouvelle étape de découverte des équipements du sous-réseau, le module de découverte (MD) met à jour les bases de données du noyau (N) et du module de configuration des modèles (MCM) contenant la liste des équipements et de leurs domaines.

[0009] Selon une autre particularité, toutes les alarmes émises par les différents modules sont envoyées à l'administrateur principal (AD) via le module de sécurisation d'alarmes (MSA), ladite alarme étant accompagnée d'un message d'envoi destiné au serveur du module de sécurisation d'alarmes (sMSA).

[0010] Selon une autre particularité, le procédé d'administration d'un réseau est composé:

- 30 - d'une étape de réception de l'alarme par l'administrateur principal (AD) et de réception dudit message d'envoi par le serveur du module de sécurisation d'alarmes (sMSA),
- d'une étape d'envoi d'un message de confirmation de réception par le serveur du module de sécurisation d'alarmes (sMSA) au client du module de sécurisation d'alarmes (cMSA),
- d'une étape de réception du message de confirmation de réception par le client du module de sécurisation d'alarmes (cMSA),
- d'une étape de mise à jour des instances d'alarmes stockées dans le module de filtrage d'alarmes (MFA).

[0011] Selon une autre particularité, lorsque le client du module de confirmation d'alarmes (MCA) n'a pas reçu le message de confirmation de réception, il renvoie, après un temps déterminé, l'alarme à l'administrateur principal (AD).

40 l'alarme étant accompagnée d'un message d'envoi destiné au serveur du module de sécurisation d'alarmes (sMSA).

[0012] Selon une autre particularité, lorsque le module de calcul d'indicateurs (MCI) ou le module de découverte (MD) n'obtient pas de réponse à une requête envoyée à un équipement du sous-réseau, le module de calcul d'indicateurs (MCI) ou le module de découverte (MD) envoie un message à un module chien de garde (MCG), le module chien de garde (MCG) interrogeant l'équipement supposé disparu et attendant de manière plus longue, une réponse.

[0013] Selon une autre particularité, lorsque, après un temps déterminé, le module chien de garde (MCG) n'obtient pas de réponse de l'équipement supposé disparu, l'équipement est supprimé de la base de données du noyau (N), de la base de données du module de découverte (MD) et de la base de données du module de configuration des domaines (MCM), le module chien de garde (MCG) envoyant une alarme à l'administrateur principal (AD), lui indiquant la disparition de l'équipement, l'alarme étant perçue par l'administrateur comme provenant de l'équipement et envoyée en utilisant le module de sécurisation.

[0014] Selon une autre particularité, lorsque le module chien de garde (MCG) obtient une réponse de l'équipement supposé disparu, il demande la redécouverte des domaines, si la demande a été émise par le module de calcul d'indicateur.

[0015] Un autre but de l'invention est de fournir un système d'administration de réseaux et de systèmes.

55 [0016] Ce but est atteint par le fait que ce système d'administration d'un réseau par un administrateur principal communiquant avec des équipements (ET) à travers un réseau grande distance (WAN) et des réseaux locaux d'entreprises (RLE) est caractérisé en ce qu'il comprend au moins un sous-administrateur (COACH) localisé sur le réseau local d'entreprise (RLE) et administré par l'administrateur principal (AD). Le sous-administrateur (COACH) comportant

des moyens d'interroger les équipements du réseau local d'entreprise (RLE), de filtrer et de stocker les alarmes lancées par les agents (snmp) fonctionnant sur les équipements du réseau, des moyens de sécuriser les alarmes envoyées à l'administrateur principal (AD) et un moyen de dialogue avec l'administrateur principal et entre les différents moyens.

5 [0017] Selon une particularité de l'invention, le moyen de dialogue est constitué d'un noyau (N) dialoguant avec l'administrateur principal (AD) et permettant le dialogue entre les différents modules composant ledit système. Selon une autre particularité, les moyens d'interroger les équipements du réseau local d'entreprise (RLE), de filtrer et de stocker les alarmes lancées par les agents (snmp) fonctionnant sur les équipements du réseau sont constitués

10 - d'un module de découverte (MD) découvrant les équipements (ET) du sous-réseau à administrer et classant lesdits équipements dans des domaines en fonction des types d'agents qui y sont installés. Ce module de découverte amplifie la fonction de découverte de l'administrateur central, par une précision accrue, une découverte plus rapide et une économie considérable en bande passante.

15 - d'un module de configuration de modèles (MCM) comportant des modèles de filtre d'alarmes et des indicateurs pouvant être instanciés sur les équipements du sous-réseau, chaque indicateur étant associé à une période d'interrogation.

20 - d'un module de calcul d'indicateurs (MCI) calculant le résultat de l'application d'un indicateur à un équipement, l'indicateur étant défini pour le domaine auquel l'équipement appartient, le résultat de cette application étant comparé à une valeur seuil ne devant pas être dépassée un certain nombre de fois, pendant un certain laps de temps.

- d'un module de filtrage d'alarmes (MFA) recevant les alarmes envoyées par les agents (snmp) fonctionnant sur les équipements du sous-réseau, puis, sélectionnant une partie desdites alarmes à l'aide d'un filtre défini pour un domaine donné, lesdites alarmes sélectionnées étant ré-émises vers l'administrateur principal (AD).

[0018] Selon une autre particularité, les moyens de sécuriser les alarmes envoyées à l'administrateur principal (AD) sont constitués :

25 - d'un module de chien de garde (MCG) qui, lorsqu'un module le lui demande, vérifie l'existence d'un équipement par l'envoi répété d'appels, si l'équipement disparu n'a pas répondu à un nombre prédéfini d'appels, ledit module chien de garde (MCG) envoie une alarme à l'administrateur principal (AD) qui sera perçue par ce dernier comme provenant de l'équipement disparu.

30 - d'un module de sécurisation d'alarmes (MSA) fonctionnant selon le mécanisme client-serveur, le client (cMSA), lors de l'envoi d'au moins une alarme à l'administrateur, attendant un message de confirmation du serveur (sMSA) localisé sur l'administrateur principal (AD), ledit serveur (SMSA), après réception dudit message d'envoi, envoyant un message de confirmation de réception au client (cMSA), le client renvoyant l'alarme et un autre message d'envoi à administrateur lorsque, après un temps déterminé, le message de confirmation de réception n'est pas reçus par le client.

[0019] Selon une autre particularité, lorsque la valeur seuil est dépassée un certain nombre de fois pendant un certain laps de temps, le module de calcul d'indicateurs (MCI) émet une alarme vers l'administrateur principal (AD), ladite alarme étant perçue par l'administrateur principal comme étant émise par l'équipement dont l'instanciation a été effectuée.

[0020] Selon une autre particularité, un indicateur est une équation appliquée à des instances d'objets d'une base de gestion d'informations (MIB), les instances étant obtenues par une interrogation des agents (SNMP) fonctionnant sur chacun des équipements du sous-réseau.

[0021] Selon une autre particularité, le résultat d'un indicateur et/ou une liste des alarmes envoyées peut être stocké dans un fichier archivé sur le disque dur.

[0022] Selon une autre particularité, le paramétrage des filtres d'alarmes s'effectue soit par un fichier d'initialisation soit via le protocole snmp.

[0023] Selon une autre particularité, les alarmes à envoyer sont accumulées par le module de confirmation d'alarmes afin de les envoyer groupées, par paquet, à une fréquence donnée.

50 [0024] Selon une autre particularité, un modèle de filtre d'alarmes contient une description de l'alarme à reconnaître et un nombre maximal d'occurrence d'alarmes avant lequel une autre alarme est émise vers l'administrateur principal (AD), si ledit nombre maximal d'occurrence d'alarmes est reçu pendant une certaine période.

[0025] Selon une autre particularité, les différents modules interrogent le noyau (N) pour initialiser leurs paramètres de fonctionnement.

55 [0026] Selon une autre particularité, le noyau (N) gère une base de données contenant toutes les instances de la base de gestion d'informations (MIB), ledit noyau comportant au moins deux supports (sockets) de communication et une interface commune de gestion de la communication avec les modules.

[0027] Selon une autre particularité, les paramètres d'initialisation du module de découverte (MD) comportent la

période espaçant deux découvertes, le nombre minimum de systèmes à découvrir et le masque du protocole internet (IP) déterminant l'étendue du réseau à découvrir.

**[0028]** Selon une autre particularité, un équipement (ET) découvert est classé dans un ou plusieurs domaines en fonction de ses réponses aux interrogations effectuées sur chaque ensemble d'instances d'objets de la base de gestion d'informations (MIB) définissant un domaine.

**[0029]** D'autres particularités et avantages de la présente invention apparaîtront plus clairement à la lecture de la description ci-après faite en référence aux dessins annexés dans lesquels :

- la figure 1 représente un exemple d'implémentation du procédé d'administration de deux sous-réseaux.
- la figure 2 représente l'architecture du système d'administration.
- la figure 3 représente un exemple d'implémentation du procédé d'administration de n sites.
- la figure 4 représente un système d'administration classique.

**[0030]** La présente invention propose un procédé et un système de gestion de réseaux totalement paramétrables à distance via un protocole standard : le protocole SNMP. Comme le montre la figure 1, le système d'administration de réseau est composé d'un administrateur (AD1) et d'au moins un sous-réseau local (RLE1, RLE2) relié à un agent ouvert central pour une administration concentrée (COACH, Central Open Agent for Concentrated Handling). Le sous-administrateur (COACH1) agit à un niveau intermédiaire d'administration. Situé sur le réseau local d'entreprises (RLE1), il permet de limiter le flux d'administration entre l'administrateur principal (AD1) et les équipements (ET) du réseau (RLE1). Il est perçu par les équipements du réseau comme un administrateur et par l'administrateur comme un équipement.

**[0031]** Le sous-administrateur (COACH), tel que représenté en figure 2, comporte un ensemble de processus aussi appelés "modules" qui dialoguent les uns avec les autres et avec l'administrateur principal (AD) par l'intermédiaire d'un processus central aussi appelé "noyau" (N). Les dialogues entre les différents modules se font par un support (socket) portable et standard. Chaque module est dédié à une fonction précise.

**[0032]** Le module central ou noyau (N) a deux fonctions principales. D'une part, il dialogue avec l'administrateur (AD) et d'autre part, il gère le dialogue entre les différents modules composant le sous-administrateur (COACH). En effet, le noyau (N) répond au dialogue (snmp), lorsque le sous-administrateur (COACH) est interrogé ou configuré par l'administrateur. Il existe deux types de dialogue avec les modules, c'est pourquoi deux supports (sockets) de communication sont souhaitables pour gérer le dialogue noyau-module. Le premier type de dialogue se fait à l'initiative du noyau et concerne les mises à jour d'instances ou les demandes d'informations sur une base de gestion d'informations (MIB) ou les transmissions de notifications provenant d'un autre module. Le second type de dialogue se fait à l'initiative des modules et concerne les demandes d'informations ou les mises à jour d'instances de la base de gestion d'informations (MIB). Le noyau gère deux listes de supports. La création de support dans chacune de ces listes se fait dynamiquement lors de la connexion des modules. Pour le dialogue (snmp) avec l'administrateur, le standard impose l'utilisation d'un seul support (socket). Le dialogue se fait sur le port 161/udp, mais l'utilisation d'un dispatcher de requêtes nécessite l'utilisation d'un autre port paramétrable afin d'avoir la possibilité de faire fonctionner plusieurs agents (snmp) sur un même équipement. Pour simplifier la gestion de communication avec les modules, une interface commune est définie sous forme de bibliothèque. Par ailleurs, le noyau (N) possède une mémoire cache (cache memory) (C) contenant toutes les informations résultant de l'administration d'un sous-réseau (RLE). Chaque module interroge le noyau pour initialiser ces paramètres de fonctionnement. En outre, le noyau (N) gère une base de données contenant toutes les instances de la base de gestion d'informations (MIB) du sous-réseau administré par le sous-administrateur (COACH).

**[0033]** Le module de découverte (MD) découvre le sous réseau (RLE1) sur lequel est installé le sous-administrateur (COACH1). A l'aide d'une table des masques d'adresse du protocole internet (IP, Internet Protocol), le module de découverte (MD) détermine les adresses (IP) des équipements (ET) que le sous-administrateur peut éventuellement administrer. Puis, le module de découverte (MD) interroge successivement par groupe de paquet internet (PING Packet Internet Groper) unitaire tous les équipements possibles. Le PING est une interrogation standard que l'on peut utiliser pour savoir si une machine est connectée sur le réseau Internet, pour déterminer la provenance d'un message ou pour vérifier si un système est toujours en activité. Lorsqu'un équipement est visible sur le réseau, il répond au PING.

**[0034]** Si un équipement est découvert, le module de découverte (MD) recherche son domaine. Chaque équipement appartient à un domaine. Le domaine de chaque équipement permet de définir des groupes d'indicateurs et de filtres d'alarme à injecter sur chacun des équipements et ceci, en fonction des agents présents sur ces équipements et donc en fonction des rôles dépourvus à chaque équipement.

**[0035]** Le domaine d'un équipement est défini selon la réponse ou non de l'équipement à un ensemble d'instances d'objets de la base de gestion d'informations (MIB snmp). Dès la découverte d'un nouvel équipement, une interrogation (polling) est effectuée sur un ensemble d'instances d'objets (snmp). Lorsqu'un équipement (ET) découvert répond aux interrogations de toutes les instances d'objets définissant un domaine, on dit que l'équipement appartient à ce domaine.

Tous les équipements découverts sont classés selon des domaines. Ces domaines permettent de différencier les différents types d'équipements et d'administrer différemment chacun des équipements selon son domaine. Un équipement peut appartenir à plusieurs domaines.

[0036] Le domaine MIB2 pourrait, par exemple, être défini par la réponse à l'instance "sysUpTime0". Tous les équipements découverts sont interrogés sur cette instance. Ceux qui y répondent appartiennent au moins au domaine MIB2.

[0037] Enfin, lorsque le module de découverte (MD) a découvert un équipement et son domaine, il envoie une notification à un module de configuration des modèles (MCM) en lui indiquant l'adresse du protocole internet (IP) de l'équipement découvert et le domaine auquel cet équipement appartient. Avantageusement, le module de découverte (MD) envoie, de plus, ces mêmes informations au noyau (N) qui les stockera dans une base de données.

[0038] Généralement, lorsqu'un système existant est découvert une seconde fois, son domaine n'est pas, à nouveau, recherché. Néanmoins, le domaine d'un système peut être recherché en positionnant sur "actif" (ON) l'instance de la base de gestion d'informations (MIB) relative à la découverte des domaines. Dans ce cas si, le domaine n'est pas le même que le précédent, la base de données du noyau est automatiquement mise à jour et des notifications sont automatiquement envoyées au module de configuration des modèles (MCM).

[0039] Lorsqu'un équipement précédemment découvert ne répond plus à un PING unitaire, le modèle de découverte (MD) envoie une notification à un module (MCG) chien de garde (Watchdog) afin qu'il vérifie si l'équipement a réellement disparu du réseau.

[0040] Dès sa connexion, le module de découverte (MD) interroge le noyau (N) afin de connaître ses paramètres d'initialisation:

- la période entre deux découvertes successives,
- le nombre minimum de systèmes à découvrir,
- le masque du protocole internet (IP) déterminant l'étendue du réseau à découvrir.

[0041] Le module de découverte comporte des éléments de configuration de base, un ensemble d'instances d'objets de la base de gestion d'information (MIB) à interroger et la liste des systèmes découverts ainsi que leurs domaines.

[0042] L'annexe 7 présente un modèle de configuration de la découverte. L'annexe 8 présente les données dynamiques de découverte.

[0043] Le module de filtrage d'alarmes (MFA) reçoit les alarmes (traps) envoyées par les agents (snmp), implémentés sur les équipements (ET) et filtre les alarmes à réémettre vers l'administrateur principal (AD). Dès la réception d'une alarme, ce module tente de reconnaître dans quel domaine appartient l'équipement (ET) qui a envoyé cette alarme. Ce renseignement lui permettra de déterminer le modèle de filtre à appliquer à cette alarme. Un modèle de filtre d'alarmes est défini par une description de l'alarme à reconnaître (champs SNMP de description: Entreprise, générique, spécifique) et par un nombre maximal d'occurrence d'alarmes pendant une certaine période avant lequel une autre alarme est émise. Le choix du modèle de filtre se fait en fonction du domaine auquel l'équipement envoyant une alarme appartient. Lorsqu'une alarme n'est pas reconnue, elle est transmise à l'administrateur principal (AD). De plus, la première instance d'alarme reçue est toujours émise vers l'administrateur principal (AD). Par exemple, pour un équipement appartenant au domaine "Imprim", c'est-à-dire une imprimante, un modèle d'alarme indiquant "plus de papier dans l'imprimante" est défini. Ce modèle est instancié sur toutes les imprimantes du sous-réseau. Le modèle de filtre de cette alarme est décrit comme une alarme de niveau 0, envoyé à l'administrateur (AD). Ainsi, si l'un des agents des imprimantes émet cette alarme, le module de filtrage d'alarmes (MFA) ne transmettra aucune de ces alarmes à l'administrateur principal (AD). Si, ces mêmes imprimantes émettent une alarme de dysfonctionnement révélant un "problème réseau" et que le modèle de filtre de cette alarme est décrit comme étant de niveau 1 sur 50 en moins de 30 minutes, signifiant qu'il faut réémettre une alarme lorsque cinquante alarmes ont été reçues en moins de trente minutes, le module de filtrage d'alarmes (MFA) réémettra pour chaque imprimante la première alarme reçue, puis 1 sur 50 dans une période de 30 minutes. Si seulement deux alarmes arrivent à au moins trente minutes d'intervalle, elles seront toutes les deux transmises.

[0044] Le module de filtrage d'alarmes (MFA) est aussi à l'écoute du noyau (N). Ce dernier lui envoie des notifications de mise à jour de modèle de filtre d'alarmes. Les données contenues dans le module de filtrage d'alarmes (MFA) sont la description des modèles et des informations sur les instanciations de ces modèles (date de la première instance d'alarme reçue, nombre d'alarmes reçues pendant la période critique).

[0045] En outre, l'envoi d'alarmes peut être archivé dans un fichier sur le disque dur par l'emploi de la fonction "set" et l'administrateur peut le récupérer avec, par exemple, un protocole de transfert de fichiers (FTP, File Transfert Protocol). Les informations ainsi archivées concernent la date, l'entreprise, le générique et le spécifique d'une alarme émise. Un envoi d'alarme peut, par exemple, être tracé sous cette forme: Nov 19 19:32 1997: 1.3.6.1.4.1.107.144:6:1. Cette information doit être interprétée sous cette forme : le 19 novembre 1997, à 19h32, une alarme d'entreprise 1.3.6.1.4.1.107.144 de type générique 6 et spécifique 1 a été émise vers l'administrateur. L'envoi d'alarmes peut aussi être archivé dans une table des masques d'alarmes. Avantageusement, l'ensemble des informations contenues dans

le message peut aussi être archivé.

[0046] L'annexe 2 présente un modèle de filtre d'alarmes. L'annexe 3 présente les données dynamiques d'un filtre d'alarmes.

[0047] Le module de calcul d'indicateur (MCI) calcule des indicateurs sur les équipements (ET) à administrer. Un indicateur est une équation dans laquelle des instances d'objets de gestion de base de d'informations (MIB snmp) sont introduites. Ces instances d'objets sont obtenues par l'interrogation (polling) sur les agents (snmp) fonctionnant sur chacun des systèmes à administrer. Le résultat de cette équation est comparé à une valeur seuil ne devant pas être dépassée un certain nombre de fois pendant un certain laps de temps. Lorsque la valeur seuil est dépassée, un certain nombre de fois pendant un certain laps de temps, une alarme est émise vers l'administrateur principal (AD).

[0048] Prenons l'exemple d'un indicateur à instancier sur les équipements du domaine MIB2 comportant une période d'interrogation de 60 secondes. Cet indicateur calcule l'utilisation de la bande passante d'une carte de réseau quelconque à l'aide de l'équation:

$$15 \quad (8 * \$-(\text{ifInOctets.1} + \text{ifOutOctets.1}) / \text{ifSpeed.1}$$

Cette équation sera calculée sur chacun des équipements du domaine MIB2 toutes les minutes. Si, sur le système "A", le résultat excède la valeur 10 au moins deux fois en cinq minutes, une alarme sera envoyée à l'administrateur principal (AD). Et cette alarme sera perçue par ce dernier comme provenant du système "A".

[0049] Un indicateur comporte des opérateurs simples tels que l'addition (+), la soustraction (-), la multiplication (\*), la division (/) et des opérateurs d'ensemble. Les opérateurs d'ensemble permettent d'appliquer un opérateur sur des séries d'instances d'indicateurs. Ainsi, l'opérateur:

- !SUM qui réalise la somme d'une série d'instances d'indicateurs,
- !MOY qui réalise une moyenne d'une série d'indicateurs,
- !MAX qui recherche la valeur maximum parmi une série d'indicateurs,
- !MIN qui recherche la valeur minimum parmi une série d'indicateurs.

Attention, les opérateurs d'ensemble sont appliqués à des systèmes et non au temps. L'annexe 9 nous décrit quelques exemples d'équations simples utilisant les opérateurs d'ensemble. De plus, un indicateur peut également comprendre un opérateur delta noté \$- et un opérateur d'indirection temporel noté &. L'opérateur delta est défini tel que, à l'instant t,  $\$-(x) = x(t) - x(t-T)$  où l'attribut x de valeur  $x(t-T)$  est recueilli à l'instant  $(t - T)$  et où la valeur  $\$-(x)$  donne la différence entre  $x(t)$  et  $x(t-T)$ .  $\$-(x)$  correspond à un delta et  $\$t$  à un delta(t). L'opérateur d'indirection temporel permet de réutiliser un calcul déjà effectué sur un équipement. Le module de calcul des instances (MCI) interroge le noyau pour initialiser ces paramètres de fonctionnement.

[0050] En fonctionnement, le module de configuration des modèles (MCM) notifie au module de calcul d'indicateurs (MCI) les modèles à instancier sur les équipements. Les données stockées dans le module de calcul d'indicateurs (MCI) sont les descriptions de modèles d'indicateurs (avec le nom du modèle), les instanciations de chacun des indicateurs et des informations de fonctionnement comme, par exemple, le dernier résultat de l'instance, la date de la prochaine interrogation de l'instance,...etc.

[0051] Le résultat de l'instanciation d'indicateurs peut être archivé d'une part dans un fichier sur le disque dur à l'aide de l'emploi de la fonction "set". L'utilisateur sélectionne nominativement les indicateurs qu'il veut journaliser (logger). Dans ce cas, l'administrateur peut le récupérer à l'aide d'un protocole de transfert de fichiers (FTP). D'autre part, le résultat de l'instanciation d'indicateurs est aussi stocké dans une table d'indicateurs accessible directement par une requête SNMP.

[0052] Les informations concernant les indicateurs ainsi archivés comportent la date, le modèle de l'indicateur interrogé, l'adresse (IP) de l'équipement interrogé et le résultat du calcul de l'indicateur. Un fichier archivé peut, par exemple, être tracé sous cette forme : Nov 27 11:44 1997:3:129.184.59.7:271.4268. Ce fichier doit être interprété sous cette forme : le 27 novembre 1997, à 11h44, l'équipement 129.184.59.7 a été interrogé sur le modèle 3 est le résultat est 271.4268.

[0053] Avantageusement, afin de limiter la taille du stockage des équations, les chaînes de caractères correspondant aux instances interrogées sont stockées dans un tableau et représentées par des identificateurs.

[0054] Remarquons que toutes les fonctions de calcul d'équations, de description de seuils, de définition de périodes de calcul, de fréquence maximale de dépassement de seuil, de sens de comparaison du résultat sont entièrement configurables à distance et dynamiquement via le protocole snmp.

[0055] L'annexe 5 présente un modèle d'indicateur. L'annexe 6 présente les données dynamiques d'indicateurs.

[0056] Lorsqu'un équipement ne répond plus aux sollicitations des modules de découvertes (MD) et de calcul d'indicateurs (MCI), le module (MCG) chien de garde (watchdog) vérifie si cette équipement a réellement disparu. En effet,

cet équipement n'a pas été forcément supprimé. Un équipement peut ne plus ne plus être visible pendant un certain laps de temps en raison des aléas liés au trafic du réseau ou parce que le réseau local d'entreprise (RLE) est surchargé. Le rôle du module chien de garde (MCG) est de le vérifier.

5 [0057] Quand, le module de découverte (MD) ou le module de calcul d'indicateurs (MCI) prévient le module chien de garde (MCG) de l'éventuelle disparition d'un équipement, le module de chien de garde (MCG) sollicite, à nouveau, cet équipement mais de manière plus pressante. Il envoie un message à l'équipement supposé disparu et attend une réponse pendant un temps très long. Il laisse beaucoup plus de temps à l'équipement pour répondre. Si l'équipement répond, le module chien de garde (MCG) ne signale rien et par défaut, les modules de découverte (MD) et/ou le module de calcul d'indicateurs (MCI) supposent que l'équipement existe toujours. Si l'équipement ne répond pas, le module chien de garde envoie un nouveau message en laissant à l'équipement supposé disparu un temps de réponse encore plus long. Après un certain nombre d'envois de messages, si l'équipement supposé disparu n'a toujours pas répondu aux différents messages, le module chien de garde (MCG) émet une alarme en direction de l'administrateur principal (AD) lui indiquant la disparition de cet équipement. Cette alarme est simulée comme provenant de l'équipement disparu. Ceci permet une valorisation de l'information et une simplification de visualisation au niveau de l'administrateur principal. Le module chien de garde (MCG) envoie des notifications au module de découverte (MD), au noyau (N) et au module de configuration des modèles (MCM) de manière à ce que l'équipement disparu soit supprimé de leurs bases de données.

20 [0058] Lorsqu'un équipement n'a pas répondu à la sollicitation du module de calcul d'indicateurs (MCI), mais que l'équipement répond à l'interrogation du module chien de garde, il est possible que des agents (snmp) aient été modifiés. Une redécouverte du domaine de ce système est alors automatiquement demandée.

25 [0059] Le module de sécurisation d'alarmes (MSA) permet de sécuriser les alarmes envoyées par le sous-administrateur (COACH) vers l'administrateur principal (AD). Ce module fonctionne selon un mécanisme client-serveur, le serveur du module de sécurisation d'alarmes (sMSA) est attaché à l'administrateur principal (AD) et le client du module de sécurisation d'alarmes est attaché au module de filtrage d'alarmes (MFA). Lorsqu'une alarme est envoyée à l'administrateur, elle est toujours accompagnée d'un message d'envoi envoyé par le client (cMSA) et destiné au serveur (sMSA). La réception de ce message d'envoi par le serveur (sMSA) implique automatiquement que l'administrateur ait reçu l'alarme accompagnant ce message. Lorsque le serveur (sMSA) réceptionne le message d'envoi, il envoie au client (cMSA) un message de confirmation de réception. Dès réception du message de confirmation de réception, le client (cMSA) enlève les instances d'alarmes stockées dans le module de filtrage d'alarmes (MFA). Lorsque, après un temps déterminé par avance, le client (cMSA) n'a pas reçu de message de confirmation de réception, il renvoie l'alarme accompagnée d'un nouveau message d'envoi à l'administrateur principal. Le client (cMSA) recommence cette opération jusqu'à ce qu'il reçoive un message de confirmation de réception.

30 [0060] La confirmation d'alarmes permet de garantir de manière quasiment absolue la réception des alarmes par l'administrateur. Le fonctionnement global a encore été amélioré par une fonction d'émission d'alarmes en bloc. Le module de sécurisation d'alarmes (MSA) a la possibilité de ne pas envoyer pas instantanément les alarmes mais les archive puis les envoie, par paquet, à une fréquence donnée. Les lignes de communication ne sont sollicitées que pendant cette période. La fréquence d'émission des alarmes est choisie lors du paramétrage du module de sécurisation d'alarmes. Ce principe est particulièrement intéressant pour les lignes du Réseau Numérique à Intégration de Service (RNIS) (Integrated Services Digital Network, ISDN) pour lesquelles l'ouverture d'une ligne prend du temps, et la fermeture s'effectue après un délai. Avantageusement, pour augmenter encore la sécurisation de ces alarmes, la ligne est ouverte quelques secondes avant l'envoi des alarmes.

35 [0061] Le module de configuration de modèles (MCM) permet d'indiquer dynamiquement aux modules de calcul d'indicateurs (MCI) et de filtre d'alarmes (MFA), les indicateurs et les modèles de filtrage d'alarmes à appliquer sur chacun des équipements (ET) du sous-réseau. Lors de la découverte d'un équipement, le module de découverte (MD) envoie une notification au module de configuration des modèles (MCM), lui indiquant l'adresse du protocole internet (adresse IP) de l'équipement découvert, ainsi que le domaine auquel il appartient. Le module de configuration des modèles (MCM) notifie, alors, l'indicateur, au module de calcul d'indicateurs (MCI) et le modèle de filtre, au module de filtrage d'alarmes.

40 [0062] Si, par exemple, un indicateur doit être instancié sur les systèmes MIB2, pour tous les systèmes découverts, le module de configuration des modèles (MCM) va indiquer l'instanciation de cet indicateur au module de calcul d'indicateurs (MCI).

[0063] Le module de configuration de modèles (MCM) comporte les correspondances entre les domaines et leurs modèles (de filtre et d'indicateur).

45 [0064] Le module de configuration de modèles (MCM) est composé d'une partie d'initialisation et d'une partie de mise à jour en fonctionnement. Lors de l'initialisation, les descriptions d'indicateurs et de modèles de filtre existant dans la base de données du noyau (N) sont détruites. Ces descriptions sont par la suite lues dans un fichier d'initialisation (confmod.ini).

[0065] Un exemple d'un fichier de configuration (confmod.ini) contenant un indicateur est décrit en annexe 4. Un

55 indicateur est défini par différents champs:

	Champ	Définition
5	<b>Type</b>	IND pour un modèle d'INDicateurs
	<b>Id</b>	Index d'indicateur (génération automatique)
	<b>Nom</b>	Nom de l'indicateur
10	<b>Domaine</b>	Regroupement d'équipements administrés trouvés par leur adresse en domaines identifiables par 5 requêtes "Get" envoyées par le sous-administrateur (COACH). Cela signifie qu'aujourd'hui, il existe au plus 5 identifiants d'objets (Oids) possibles pour définir un domaine
15	<b>Equation</b>	Equation de l'indicateur
	<b>T polling</b>	Période d'interrogation ou de construction de l'indicateur
20	<b>Seuil</b>	Seuil de décision pour l'émission d'une alarme
	<b>Apparition</b>	Nombre d'apparitions de la valeur seuil après laquelle il y a émission d'alarmes
25	<b>Période</b>	Période au-delà de laquelle le nombre d'apparitions des x valeurs de seuil est remis à zéro
	<b>Sens de comparaison</b>	Sens de comparaison entre le seuil défini et le résultat de l'équation pour décrire un dépassement. Il peut être >, <, =, ou !=
30	<b>Booleen de Log de l'indicateur</b>	Ce champ permet de créer un historique (logguer) sur l'indicateur en phase de journalisation générale. Il prend la valeur "LOG" pour logguer l'indicateur ou "NLOG" pour ne jamais logguer l'indicateur

35 [0066] Un exemple d'un fichier de configuration (confmod.ini) contenant un modèle de filtre d'alarmes est décrit en annexe 1. Un modèle de filtre d'alarmes est défini par différents champs:

	Champ	Définition
40	<b>Type</b>	FIL pour un modèle de FILtre
	<b>Id</b>	Index du modèle de filtre (génération automatique)
	<b>Nom</b>	Nom du filtre
45	<b>Domaine</b>	Regroupement des équipements administrés trouvés par leur adresse en domaines identifiable par 5 requêtes "Get" envoyées par le sous-administrateur COACH
	<b>Enterprise</b>	Champ "enterprise" de l'alarme à filtrer
	<b>Generic</b>	Champ "générique" de l'alarme à filtrer
	<b>Specific</b>	Champ "spécifique" de l'alarme à filtrer
50	<b>Apparition</b>	Nombre d'apparitions de l'alarme après laquelle, il y a réémission d'une alarme vers l'administrateur
	<b>Période</b>	Période au-delà de laquelle sans réception d'alarmes de ce type, le nombre d'apparition d'alarmes est remis à zéro.

55 [0067] Après initialisation, le module de configuration des modèles (MCM) interroge le noyau afin de connaître tous les équipements découverts ainsi que leurs domaines. Puis, il envoie des notifications au module de filtrage d'alarmes

(MFA) et au module de calcul d'indicateurs (MCI), leur indiquant les modèles à instancier selon les adresses du protocole internet (adresse IP) des équipements découverts.

5 [0068] En fonctionnement courant, le module de configuration des modèles (MCM) est à l'écoute du support (socket) de communication du noyau et attend des changements. Ces changements peuvent concerner soit l'ajout ou la suppression d'un équipement sur le réseau, soit des modifications d'indicateurs ou de modèles de filtre.

[0069] D'autres modifications à la portée de l'homme de métier font également partie de l'esprit de l'invention.

10

15

20

25

30

35

40

45

50

55

## ANNEXE 1

5

10 # SECTION de description des filtres de traps

15 #

# Format de la ligne de description

15 # | Type | nom du trap | entreprise | Generic | Specific | limite en nb traps | période |

20 #

# AXA/COACH/unix/trapFilters

25 #

FIL 1 alix-fs-nfull 2 Bull. 118 6 4 1 60

25 FIL 2 alix-fs-error 2 1.3.6.1.4.1.107.114 6 5 100 6

30 FIL 3 alix-uxLoginSession-setFailed 2 Bull. 118 6 33 3 30

30 FIL 4 trap\_essai\_4 1 1.3.6.1.4.1.107.144 6 7 3 10

35 FIL 5 trap\_essai\_5 1 1.3.6.1.4.1.107.144 6 8 2 10

35 FIL 6 alix-fs-nfull 2 Bull. 118 6 9 1 60

40 FIL 7 alix-fs-error 2 Bull. 118 6 10 1 60

40 FIL 8 alix-uxLoginSession-setFailed 2 Bull. 118 6 11 3 30

45 FIL 9 trap\_essai\_4 1 1.3.6.1.4.1.107.144 6 12 3 10

45 FIL 10 trap\_essai\_5 1 1.3.6.1.4.1.107.144 6 13 2 10

50 FIL 11 alix-fs-nfull 2 Bull. 118 6 14 1 60

50 FIL 12alix\_fs\_error 2 Bull. 118 6 15 1 60

55 FIL 13 alix-uxLoginSession-setFailed 2 Bull. 118 6 133 3 30

55 FIL 14 trap\_essai\_4 1 1.3.6.1.4.1.107.144 6 17 3 10

55 FIL 15 trap\_essai\_5 1 1.3.6.1.4.1.107.144 6 18 2 10

55 FIL 16 alix-fs-nfull 2 Bull. 118 6 19 1 60

55 FIL 17 alix\_fs\_error 2 Bull. 118 6 20 1 60

55 FIL 18 alix-uxLoginSession-SetFailed 2 Bull. 118 6 211 3 30

55 FIL 19 trap\_essai\_4 1 1.3.6.1.4.1.107.144 6 212 3 10

5 FIL 20 trap\_essai\_5 1 1.3.6.1.4.1.107.144 6 213 2 10  
FIL 21 alix\_fs\_nfull 2 Bull. 118 6 24 1 60  
FIL 22 alix-fs-error 2 Bull. 118 6 25 1 60  
FIL 23 alix-uxLoginSession-setFailed 2 Bull. 118 6 233 3 30  
10 FIL 24 trap\_essai\_4 1 1.3.6.1.4.1.107.144 6 27 3 10  
FIL 25 trap\_essai\_5 1 1.3.6.1.4.1.107.144 6 28 2 10  
FIL 26 alix-fs-nfull 2 Bull. 118 6 29 1 60  
15 FIL 27 alix-fs-error 2 Bull. 118 6 30 1 60  
FIL 28 alix-uxLoginSession-setFailed 2 Bull. 118 6 311 3 30  
20 FIL 29 trap\_essai\_4 1 1.3.6.1.4.1.107.144 6 312 3 10  
FIL 30 trap\_essai\_5 1 1.3.6.1.4.1.107.144 6 313 2 10

25

30

35

40

45

50

55

## ANNEXE 2

5

-- Modeles de filtres

10

cfgFilterTable OBJECT-TYPE  
 15           SYNTAX SEQUENCE OF CfgFilterEntry  
           ACCESS not-accessible  
           STATUS mandatory  
           DESCRIPTION  
             "Table de configuration des modeles de filtres."  
 20           ::= { CoachCfg 2 }

cfgFilterEntry OBJECT-TYPE  
 25           SYNTAX CfgFilterEntry  
           ACCESS not-accessible  
           STATUS mandatory  
           DESCRIPTION  
             "Une entree (ligne) dans la table des modeles de filtres."  
 30           INDEX { cfgFilterId }  
           ::= { cfgFilterTable 1 }

CfgFilterEntry ::=  
 35           SEQUENCE {  
             cfgFilterId  
             INTEGER,  
             cfgFilterLabel  
             OCTET STRING,  
 40           cfgFilterDomain  
             INTEGER,  
             cfgFilterEnterprise  
             OBJECT IDENTIFIER,  
 45           cfgFilterGeneric  
             INTEGER,  
             cfgFilterspecific  
             INTEGER,  
 50           cfgFilterCptMax  
             INTEGER,  
             cfgFilterPeriodValid  
             INTEGER  
           }  
 55

```

5           cfgFilterId OBJECT-TYPE
           SYNTAX INTEGER
           ACCESS read-only
           STATUS mandatory
           DESCRIPTION
10          "La valeur de cet attribut identifie de maniere unique une entree dans
           la table des modeles de filtres."
           ::= { cfgFilterEntry 1 }

15           cfgFilterLabel OBJECT-TYPE
           SYNTAX OCTET STRING
           ACCESS read-write
           STATUS mandatory
           DESCRIPTION
20          "Description textuelle d'un modele de filtre."
           ::= { cfgFilterEntry 2 }

25           cfgFilterDomain OBJECT-TYPE
           SYNTAX INTEGER
           ACCESS read-write
           STATUS mandatory
           DESCRIPTION
30          "Identifiant du domaine auquel appartient le modele de filtre."
           ::= { cfgFilterEntry 3 }

35           cfgFilterEnterprise OBJECT-TYPE
           SYNTAX OCTET STRING
           ACCESS read-write
           STATUS mandatory
           DESCRIPTION
40          "Object Identifier de l'entreprise du trap."
           ::= { cfgFilterEntry 4 }

45           cfgFilterGeneric OBJECT-TYPE
           SYNTAX INTEGER
           ACCESS read-write
           STATUS mandatory
           DESCRIPTION
50          "Numero generique du trap."
           ::= { cfgFilterEntry 5 }

55           cfgFilterSpecific OBJECT-TYPE
           SYNTAX INTEGER
           ACCESS read-write
           STATUS mandatory

```

5           **DESCRIPTION**

      "Numero specifique du trap."

      ::= { cfgFilterEntry 6 }

10

15           **cfgFilterCptMax OBJECT-TYPE**

      SYNTAX INTEGER

      ACCESS read-write

      STATUS mandatory

20           **DESCRIPTION**

      "Nombre de fois ou le trap doit etre recu durant <cfgFilterPeriodValid>  
      pour qu'il soit transmis."

25

      ::= { cfgFilterEntry 7 }

30

35           **cfgFilterPeriodValid OBJECT-TYPE**

      SYNTAX INTEGER

      ACCESS read-write

      STATUS mandatory

40           **DESCRIPTION**

      "Periode (en secondes) durant laquelle le trap doit etre recu  
      <cfgFilterCptMax> fois pour etre transmis."

45

      ::= { cfgFilterEntry 8 }

50

55

40

45

50

55

## ANNEXE 3

5

-- Donnees de filtres

10 filterTable OBJECT-TYPE  
 SYNTAX SEQUENCE OF FilterEntry  
 ACCESS not-accessible  
 STATUS mandatory  
 DESCRIPTION  
 "Table associant un modele de filtre a une machine."  
 ::= { CoachData 2 }

20 filterEntry OBJECT-TYPE  
 SYNTAX FilterEntry  
 ACCESS not-accessible  
 STATUS mandatory  
 DESCRIPTION  
 "Une entree (ligne dans la table des filtres.)"  
 25 INDEX { filterId,filterIpAddress }  
 ::= { filterTable 1 }

30 FilterEntry ::=  
 SEQUENCE {  
 filterId  
 INTEGER,  
 filterIpAddress  
 IpAddress  
 }

40 filterId OBJECT-TYPE  
 SYNTAX INTEGER  
 ACCESS read-only  
 STATUS mandatory  
 45 DESCRIPTION  
 "Identifiant du filtre (le meme que <cfgFilterId>), la valeur de cet  
 attribut identifie de maniere unique avec <filterIpAddress> une entree  
 dans la table des filtres."  
 50 ::= { filterEntry 1 }

55

5 filterIpAddress OBJECT-TYPE

SYNTAX IpAddress

ACCESS read-only

STATUS mandatory

DESCRIPTION

10 "Adresse IP de la machine émettrice du trap, la valeur de cet attribut identifie de manière unique avec <filterId> une entrée dans la table des filtres."

15 ::= { filterEntry 2 }

20

25

30

35

40

45

50

55

## ANNEXE 4

5

# SECTION de description des indicateurs

#

10

# type : IND | FIL respectivement INDicateurs ou FILtre

# Id : index d'indicateur (génération automatique)

15

# Nom : nom de l'indicateur

# Domaine : regroupement de systèmes managés trouvés par leur  
adresse en domaines identifiables par 5 requêtes get  
envoyées par COACH

20

# Equation : équation de l'indicateur

# T polling : période de polling ou de construction de l'indicateur

25

# Seuil : seuil de décision pour l'émission d'un trap

# Apparition : nombre d'apparitions de la valeur de seuil après laquelle,  
il y a émission de traps

30

# Période : sur quelle période apparaissent les x valeurs de seuil

# Sens de comparaison : sens de comparaison entre le seuil et le résultat

35

# Log : indique si l'indicateur devra être loggué ou non

#

40

# Format de la ligne de description

# | type | Id | Nom | Domaine | Equation | T polling | seuil | x fois | en T secondes |  
sens du test | log

45

#

# AXA/COACH/internet/indicators

50

#

# % d'utilisation de la bande passante sur l'interface

55

```

5      IND 1 ifUtilizationBandWith 2(((8*$(ifInOctets.1+ifOutOctets.1))/$t)/ifSpeed.1)*100
600 10 1 1200 > LOG

# % d'utilisation de la bande passante sur le segment
10     IND 2 ifUtilizationBandWithAll 3 | SUM(ifUtilizationBandWith) 1210 10 1 3 3600 >
LOG

# Debit de réjection de paquets en entrée et sortie sur le segment
15     IND 3 ifDiscards 2 $(ifInDiscards.1+ifOutDiscards.1) 120 1 1 120 > LOG

# Somme des débits de réjection de paquets en entrée et sortie sur le segment
IND 4 ifDiscardsAll 3 | SUM(ifDiscards) 320 3 1 320 > LOG

# Longueur de la file d'attente des paquets en sortie sur l'interface
15     IND 5 coachIfOutQlen 2 ifOutQLen.1 330 5 1 330 > LOG

# Somme des Longueurs de la file d'attente des paquets en sortie sur toutes les interfaces
20     du segment
IND 6 coachIfOutQLenAll 3 | SUM(coachIfOutQLen) 670 50 1 670 > LOG

# Nombre de paquets retransmis sur l'interface
25     IND 7 coachcpRetransSegs 2 tcpRetransSegs.0 340 5 1 340 > LOG

# Débit d'erreurs sur l'interface
30     IND 8 ifErrors 2 $(ifInErrors.1+ifOutErrors.1)$t 290 5 1 290 > LOG

# Débit d'erreurs sur le segment
35     IND 9 ifErrorsSUM 3 !SUM(ifErrors) 620 2 1 620 > LOG

# Débit moyen d'erreurs sur toutes les interfaces du segment
IND 10 ifErrorsMOY 3 !MOY(ifErrors)*100 630 5 1 630 > LOG

# Débit unicast sur l'interface en entrée et en sortie
40     IND 11 ifUcastPackets 2 (ifInUcastPkts.1+ifOutUcastPkts.1)$t 280 5 1 280 > LOG

# Débit multicast sur l'interface en entrée et en sortie
45     IND 12 ifNUPackets 2 (ifInNUcastPkts.1+ifOutNUcastPkts.1)$t 280 5 1 280 > NLOG

# % d'erreurs sur l'interface par rapport au total des paquets émis ou reçus
IND 13 ifErrorsRatio 2 (&ifErrors/(&ifInPackets+&ifOutPackets)) *100 570 5 1570 >
NLOG

# % moyen sur le segment des erreurs sur toutes les interfaces du segment
50     IND 14 ifErrorsRatioLinkMOY 3 !MOY(ifErrorsRatio) 1220 5 1 1220 > LOG

```

```

# % Somme des pourcentages d'erreurs sur toutes les interfaces des liens
IND 15 IfErrorsRatioLinkSUM 3 !SUM(ifErrorsRatio) 1220 20 1 1220 > LOG

5 # Quantité d'erreurs d'en-tête et d'adresse sur l'interface. Utiliser pour calculer
ipInputErrorsPercent
IND 16 ipInputErrors 2$-(ipInHdrErrors.0+ipInAddrErrors.0) 650 5 1 650 > LOG

10 # % d'erreurs d'en-tête et d'adresse sur l'interface
IND 17 ipInputErrorsPercent 2 (&ipInputErrors/($-(ipInDelivers.0)))*100 650 5 1 650
> LOG

15 # Somme des pourcentages d'erreurs d'en-tête et d'adresse sur l'interface
IND 18 ipInputErrorsPercentOnLink 3 !SUM(ipInputErrorsPercent) 300 5 1 300 > LOG

# Indisponibilité d'une machine
20 IND 19 NoDisponibility 2-$t/($-(sysUpTime.0)) 100 1 1 300 > LOG

# Somme de l'indisponibilité pour l'ensemble des machines du segment
IND 20 NoDisponibilityOnLink 3 !SUM(NoDisponibility) 150 100 1 300 > LOG

25 # 21/10/97 20:17 fichier : CONFMOD DOC#version DRAFT

```

30

35

40

45

50

55

## ANNEXE 5

5

10

Coach-MTB DEFINITIONS ::= BEGIN

15

bull OBJECT IDENTIFIER ::= { enterprises 107 }  
 gam OBJECT IDENTIFIER ::= { bull 146 }  
 Coach OBJECT IDENTIFIER ::= { gam 1 }  
 CoachCfg OBJECT IDENTIFIER ::= { Coach 1 }  
 20 CoachData OBJECT IDENTIFIER ::= { Coach 2 }  
 CoachSystem OBJECT IDENTIFIER ::= { Coach 3 }

25

-- =====  
-- Configuration de Coach  
-- =====

30

-- Modeles d'indicateurs

35

cfgIndicatorTable OBJECT-TYPE  
 SYNTAX SEQUENCE OF CfgIndicatorEntry  
 ACCESS not-accessible  
 STATUS mandatory  
 DESCRIPTION  
 "Table de configuration des modeles d'indicateurs."  
 ::= { CoachCfg 1 }

40

cfgIndicatorEntry OBJECT-TYPE  
 SYNTAX CfgIndicatorEntry  
 ACCESS not-accessible  
 STATUS mandatory  
 DESCRIPTION  
 "Une entree (ligne) dans la table des modeles d'indicateurs."  
 INDEX { cfgIndicatorId }  
 ::= { cfgIndicatorTable 1 }

55

```

ComparaisonType ::= INTEGER {equal(0),less(1),greater(2)}
```

5

```

CfgIndicatorEntry ::=
```

10

```

SEQUENCE {
    cfgIndicatorId
        INTEGER,
    cfgIndicatorLabel
        OCTET STRING,
    cfgIndicatorDomain
        INTEGER,
    cfgIndicatorEquation
        OCTET STRING,
    cfgIndicatorPeriodPolling
        INTEGER,
    cfgIndicatorThreshold
        INTEGER,
    cfgIndicatorCptMax
        INTEGER,
    cfgIndicatorPeriodValid
        INTEGER,
    cfgIndicatorComparaison
        ComparaisonType
}
```

20

```

25
```

30

```

cfgIndicatorId OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "La valeur de cet attribut identifie de maniere unique une entree dans
        la table des modeles d'indicateurs."
    ::= { cfgIndicatorEntry 1 }
```

35

```

40
```

```

cfgIndicatorLabel OBJECT-TYPE
    SYNTAX OCTET STRING
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "Description textuelle d'un modele d'indicateur."
    ::= { cfgIndicatorEntry 2 }
```

45

```

50
```

```

cfgIndicatorDomain OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-write
    STATUS mandatory
```

55

## DESCRIPTION

"Identifiant du domaine auquel appartient le modele d'indicateur."

::= { cfgIndicatorEntry 3 }

## cfgIndicatorEquation OBJECT-TYPE

SYNTAX OCTET STRING

10 ACCESS read-write  
STATUS mandatory  
DESCRIPTION

"Equation arithmetique decrivant le modele d'indicateur"

15 ::= { cfgIndicatorEntry 4 }

## cfgIndicatorPeriodPolling OBJECT-TYPE

SYNTAX INTEGER

20 ACCESS read-write  
STATUS mandatory  
DESCRIPTION

"Periode (en secondes) a laquelle l'indicateur va etre calcule."

25 ::= { cfgIndicatorEntry 5 }

## cfgIndicatorThreshold OBJECT-TYPE

SYNTAX INTEGER

30 ACCESS read-write  
STATUS mandatory  
DESCRIPTION

"Seuil que doit depasser l'indicateur <cfgIndicatorCptMax> fois durant <cfgIndicatorPeriodValid> pour qu'une alarme soit envoyee."

35 ::= { cfgIndicatorEntry 6 }

## cfgIndicatorCptMax OBJECT-TYPE

SYNTAX INTEGER

40 ACCESS read-write  
STATUS mandatory  
DESCRIPTION

"Nombre de fois ou l'indicateur doit depasser <cfgIndicatorThreshold> durant <cfgIndicatorPeriodValid> pour qu'une alarme soit envoyee."

45 ::= { cfgIndicatorEntry 7 }

## cfgIndicatorPeriodValid OBJECT-TYPE

SYNTAX INTEGER

50 ACCESS read-write  
STATUS mandatory  
DESCRIPTION

"Periode (en secondes) durant laquelle l'indicateur doit depasser <cfgIndicatorCptMax> fois <cfgIndicatorThreshold> pour qu'une alarme

55

soit envoyee."

::= { cfgIndicatorEntry 8 }

5

cfgIndicatorComparaison OBJECT-TYPE

SYNTAX ComparaisonType

ACCESS read-write

STATUS mandatory

DESCRIPTION

"Type de comparaison entre le seuil <cfgIndicatorThreshold> et  
le resultat de l'equation <indicatorResult> "

::= { cfgIndicatorEntry 9 }

10

15

20

25

30

35

40

45

50

55

## ANNEXE 6

5

-- Donnees d'indicateurs

10 indicatorTable OBJECT-TYPE  
 SYNTAX SEQUENCE OF IndicatorEntry  
 ACCESS not-accessible  
 STATUS mandatory  
 DESCRIPTION  
 "Table de resultats de calculs d'indicateurs."  
 ::= { CoachData 1 }

15 indicatorEntry OBJECT-TYPE  
 SYNTAX IndicatorEntry  
 ACCESS not-accessible  
 STATUS mandatory  
 DESCRIPTION  
 "Une entree (ligne) dans la table des indicateurs."  
 INDEX { indicatorId, indicatorIpAddress }  
 ::= { indicatorTable 1 }

20 IndicatorEntry ::=  
 SEQUENCE {  
 indicatorId  
 INTEGER,  
 indicatorIpAddress  
 IpAddress,  
 indicatorResult  
 INTEGER  
 }

25

30 indicatorId OBJECT-TYPE  
 SYNTAX INTEGER  
 ACCESS read-only  
 STATUS mandatory  
 DESCRIPTION  
 "Identifiant de l'indicateur (le meme que <cfgIndicatorId>), la valeur  
 de cet attribut identifie de maniere unique avec <indicatorIpAddress>  
 une entree dans la table des indicateurs."  
 ::= { indicatorEntry 1 }

35

40 indicatorIpAddress OBJECT-TYPE  
 SYNTAX IpAddress

45

50

55

5  
ACCESS read-only  
STATUS mandatory  
DESCRIPTION

10  
"Adresse IP de la machine sur lequel l'indicateur est calcule, la valeur  
de cet attribut identifie de maniere unique avec <indicatorId> une  
entree dans la table des indicateurs."  
 ::= { indicatorEntry 2 }

15  
indicatorResult OBJECT-TYPE

SYNTAX INTEGER  
ACCESS read-only  
STATUS mandatory  
DESCRIPTION  
"Resultat du calcul de l'indicateur."  
 ::= { indicatorEntry 3 }

20

25

30

35

40

45

50

55

## ANNEXE 7

5

-- Configuration de la decouverte

```

10 cfgDiscovery          OBJECT IDENTIFIER ::= { CoachCfg 4 }

15 cfgDiscoverPeriod OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "Periode (en secondes) a laquelle une decouverte est declenchee."
        ::= { cfgDiscovery 1 }

20

25 cfgDiscoverPeriodICMP OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "Periode (en secondes) de l'ICMP renforce."
        ::= { cfgDiscovery 2 }

30

35 cfgDiscoverBroadcast OBJECT-TYPE
    SYNTAX IpAddress
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "Adresse broadcast du sous-reseau."
        ::= { cfgDiscovery 3 }

40

45 cfgDiscoverDomainAtNextTime OBJECT-TYPE
    SYNTAX INTEGER {
        yes (1),
        no (2)
    }
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "Redecouverte ou non des domaines au prochain Discovery."
        ::= { cfgDiscovery 4 }

50

55

```

5                   cfgDiscoverMaxDisc OBJECT-TYPE  
10                    SYNTAX INTEGER  
11                    ACCESS read-write  
12                    STATUS mandatory  
13                    DESCRIPTION  
14                    "Nombre maximum de mauvaises decouvertes."  
15                    ::= { cfgDiscovery 5 }

15                   cfgDiscoverMaxICMP OBJECT-TYPE  
20                    SYNTAX INTEGER  
21                    ACCESS read-write  
22                    STATUS mandatory  
23                    DESCRIPTION  
24                    "Nombre maximum de mauvaises reponses ICMP."  
25                    ::= { cfgDiscovery 6 }

25                   cfgDiscoverMinMachine OBJECT-TYPE  
30                    SYNTAX INTEGER  
31                    ACCESS read-write  
32                    STATUS mandatory  
33                    DESCRIPTION  
34                    "Nombre minimum de machines sur le sous-reseau."  
35                    ::= { cfgDiscovery 7 }

35                   cfgDiscoverTimeOut OBJECT-TYPE  
40                    SYNTAX INTEGER  
41                    ACCESS read-write  
42                    STATUS mandatory  
43                    DESCRIPTION  
44                    "Time\_out de l'envoi ICMP"  
45                    ::= { cfgDiscovery 8 }

45                   cfgDiscoverTimeOutICMP OBJECT-TYPE  
50                    SYNTAX INTEGER {  
51                    yes (1),  
52                    no (2)  
53                    }  
54                    ACCESS read-write

5 STATUS mandatory

DESCRIPTION

5 "Politique ICMP renforce lors de depassement de time\_out."  
::= { cfgDiscovery 9 }

10

15

20

25

30

35

40

45

50

55

## ANNEXE 8

5

-- Donnees de decouverte

10

discoverTable OBJECT-TYPE  
 SYNTAX SEQUENCE OF DiscoverEntry  
 ACCESS not-accessible  
 STATUS mandatory  
 DESCRIPTION  
 "Table de decouverte des machines gerees par Coach."  
 ::= { CoachData 3 }

15

20

discoverEntry OBJECT-TYPE  
 SYNTAX DiscoverEntry  
 ACCESS not-accessible  
 STATUS mandatory  
 DESCRIPTION  
 "Une entree (ligne) dans la table de decouverte."  
 INDEX { discoverIpAddress }  
 ::= { discoverTable 1 }

30

35

DiscoverEntry ::=  
 SEQUENCE {  
 discoverIpAddress  
 IpAddress,  
 discoverDomainId  
 INTEGER  
 }

40

45

discoverIpAddress OBJECT-TYPE  
 SYNTAX IpAddress  
 ACCESS read-write  
 STATUS mandatory  
 DESCRIPTION  
 "Adresse IP de la machine, la valeur de cet attribut identifie de  
 maniere unique une entree dans la table de decouverte."  
 ::= { discoverEntry 1 }

50

55

discoverDomainId OBJECT-TYPE  
 SYNTAX INTEGER  
 ACCESS read-write  
 STATUS mandatory

**DESCRIPTION**

"Identifiant du domaine auquel appartient la machine."

5 ::= { discoverEntry 2 }

10

15

20

25

30

35

40

45

50

55

## [0070] ANNEXE 9

5	<b>X1 = !SUM (A)</b>	La somme X1 est réalisée sur toutes les instances A calculées par COACH. On obtient : $X1 = A1 + A2 + A3 + A4$
10	<b>X2 = !MOY(A)- !MOY(B) + !SUM(C)</b>	On obtient : $X2 = (A1 + A2 + A3 + A4)/4 + (B1 + B2 + B3 + B4)/4 + (C1 + C2 + C3 + C4)$
15	<b>X3 = !MOY(A)- !MOY(B)</b>	On obtient $X3 = (A1 + A2 + A3 + A4)/4 - (B1 + B2 + B3 + B4)/4$
20	<b>X4 = !MAX(C)</b>	On obtient la valeur maximale des valeurs des indicateurs C sur toutes les machines sur lesquelles cet indicateur est instancié. $X4 = MAX(C1, C2, C3, C4)$
25	<b>X5 = !MIN(C)</b>	On obtient la valeur minimale des valeurs des indicateurs C sur toutes les machines sur lesquelles cet indicateur est instancié.
30	<b>X5 = MIN(C1, C2, C3, C4)</b>	

## 35 Revendications

1. Procédé d'administration d'un réseau et d'un système caractérisé en ce qu'il comprend au moins un sous-administrateur (COACH) situé dans l'arbre de contenance entre un administrateur principal (AD) et les équipements du réseau, le sous-administrateur étant localisé sur le réseau local d'entreprise (RLE), administrant un sous-réseau et comprenant différents modules qui communiquent entre eux et avec un administrateur principal (AD) par l'intermédiaire d'un noyau (N), les modules interrogeant les équipements du sous-réseau et recevant les alarmes lancées par les agents (SNMP) fonctionnant sur les équipements du sous-réseau, le procédé étant composé de plusieurs étapes :
  - une étape pendant laquelle un module de découverte (MD) interroge tous les équipements (ET) possibles du sous-réseau.
  - une étape de recherche de domaine par le module de découverte (MD), lorsqu'un équipement répond à l'interrogation (SNMP),
  - une étape pendant laquelle le module de découverte (MD) envoie une notification à un module de configuration des modèles (MCM) lui indiquant l'adresse internet (IP) de l'équipement découvert et le domaine auquel l'équipement découvert appartient.
  - une étape pendant laquelle le module de configuration des modèles (MCM) notifie à un module de calcul d'indicateurs (MCI), l'indicateur à instancier sur l'équipement et à un module de filtrage d'alarmes (MFA) le modèle de filtre à instancier sur l'équipement.
2. Procédé d'administration d'un réseau et d'un système selon la revendication 1, caractérisé en ce qu'à chaque nouvelle étape de découverte des équipements du sous-réseau, le module de découverte (MD) met à jour les bases de données du noyau (N) et du module de configuration des modèles (MCM) contenant la liste des équi-

gements et de leurs domaines.

3. Procédé d'administration d'un réseau et d'un système selon la revendication 1, caractérisé en ce que toutes les alarmes émises par les différents modules sont envoyées à l'administrateur principal (AD) via le module de sécurisation d'alarmes (MSA), ladite alarme étant accompagnée d'un message d'envoi destiné au serveur du module de sécurisation d'alarmes (sMSA).
4. Procédé d'administration d'un réseau et d'un système selon la revendication 3, caractérisé en ce qu'il est composé :
  - d'une étape de réception de l'alarme par l'administrateur principal (AD) et de réception dudit message d'envoi par le serveur du module de sécurisation d'alarmes (sMSA)..
  - d'une étape d'envoi d'un message de confirmation de réception par le serveur du module de sécurisation d'alarmes (sMSA) au client du module de sécurisation d'alarmes (cMSA),
  - d'une étape de réception du message de confirmation de réception par le client du module de sécurisation d'alarmes (cMSA),
  - d'une étape de mise à jour des instances d'alarmes stockées dans le module de filtrage d'alarmes (MFA).
5. Procédé d'administration d'un réseau et d'un système selon la revendication 1, caractérisé en ce lorsque le client du module de confirmation d'alarmes (MCA) n'a pas reçu le message de confirmation de réception, il renvoie, après un temps déterminé, l'alarme à l'administrateur principal (AD), l'alarme étant accompagnée d'un message d'envoi destiné au serveur du module de sécurisation d'alarmes (sMSA).
6. Procédé d'administration d'un réseau et d'un système selon la revendication 1, caractérisé en ce lorsque le module de calcul d'indicateurs (MCI) ou le module de découverte (MD) n'obtient pas de réponse à une requête envoyée à un équipement du sous-réseau, le module de calcul d'indicateurs (MCI) ou le module de découverte (MD) envoie un message à un module chien de garde (MCG), le module chien de garde (MCG) interrogeant l'équipement supposé disparu et attendant de manière plus longue, une réponse.
7. Procédé d'administration d'un réseau et d'un système selon la revendication 6, caractérisé en ce lorsque, après un temps déterminé, le module chien de garde (MCG) n'obtient pas de réponse de l'équipement supposé disparu, l'équipement est supprimé de la base de données du noyau (N), de la base de données du module de découverte (MD) et de la base de données du module de configuration des domaines (MCM), le module chien de garde (MCG) envoyant une alarme à l'administrateur principal (AD), lui indiquant la disparition de l'équipement, l'alarme étant perçue par l'administrateur comme provenant de l'équipement à travers le module de sécurisation et envoyée en utilisant le module de sécurisation.
8. Procédé d'administration d'un réseau et d'un système selon la revendication 6, caractérisé en ce lorsque le module chien de garde (MCG) obtient une réponse de l'équipement supposé disparu, il demande la redécouverte des domaines si la demande a été émise par le module de calcul d'indicateur.
9. Système d'administration d'un réseau et d'un système par un administrateur principal communiquant avec des équipements (ET) à travers un réseau grande distance (WAN) et des réseaux locaux d'entreprises (RLE) caractérisé en ce qu'il comprend au moins un sous-administrateur (COACH) localisé sur le réseau local d'entreprise (RLE) et administré par l'administrateur principal (AD), le sous-administrateur (COACH) comportant des moyens d'interroger les équipements du réseau local d'entreprise (RLE), de filtrer et de stocker les alarmes lancées par les agents (snmp) fonctionnant sur les équipements du réseau, des moyens de sécuriser les alarmes envoyées à l'administrateur principal (AD) et un moyen de dialogue avec l'administrateur principal et entre les différents moyens.
10. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que le moyen de dialogue est constitué d'un noyau (N) dialoguant avec l'administrateur principal (AD) et permettant le dialogue entre les différents modules composant ledit système.
11. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que les moyens d'interroger les équipements du réseau local d'entreprise (RLE), de filtrer et de stocker les alarmes lancées par les agents (snmp) fonctionnant sur les équipements du réseau sont constitués
  - d'un module de découverte (MD) découvrant les équipements (ET) du sous-réseau à administrer et classant

lesdits équipements dans des domaines en fonction des types d'agents qui y sont installés. Ce module de découverte amplifie la fonction de découverte de l'administrateur central, par une précision accrue, une découverte plus rapide et une économie considérable en bande passante.

- d'un module de configuration de modèles (MCM) comportant des modèles de filtre d'alarmes et des indicateurs pouvant être automatiquement instanciés sur les équipements du sous-réseau, chaque indicateur étant associé à une période d'interrogation.
- d'un module de calcul d'indicateurs (MCI) calculant le résultat de l'application d'un indicateur à un équipement, l'indicateur étant défini pour le domaine auquel l'équipement appartient, le résultat de cette application étant comparé à une valeur seuil ne devant pas être dépassée un certain nombre de fois, pendant un certain laps de temps.
- d'un module de filtrage d'alarmes (MFA) recevant les alarmes envoyées par les agents (snmp) fonctionnant sur les équipements du sous-réseau, puis, sélectionnant une partie desdites alarmes à l'aide d'un filtre défini pour un domaine donné, lesdites alarmes sélectionnées étant ré-émises vers l'administrateur principal (AD).

15 12. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que les moyens de sécuriser les alarmes envoyées à l'administrateur principal (AD) sont constitués :

- d'un module de chien de garde (MCG) qui, lorsqu'un module le lui demande, vérifie l'existence d'un équipement par l'envoi répété d'appels, si l'équipement disparu n'a pas répondu à un nombre prédéfini d'appels, ledit module chien de garde (MCG) envoie une alarme à l'administrateur principal (AD) qui sera perçue par ce dernier comme provenant de l'équipement disparu.
- d'un module de sécurisation d'alarmes (MSA) fonctionnant selon le mécanisme client-serveur, le client (cMSA), lors de l'envoi d'au moins une alarme à l'administrateur, attendant un message de confirmation du serveur (sMSA) localisé sur l'administrateur principal (AD), ledit serveur (sMSA), après réception dudit message d'envoi, envoyant un message de confirmation de réception au client (cMSA), le client renvoyant l'alarme et un autre message d'envoi à administrateur lorsque, après un temps déterminé, le message de confirmation de réception n'est pas réceptionné par le client.

30 13. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que lorsque la valeur seuil est dépassée un certain nombre de fois pendant un certain laps de temps, le module de calcul d'indicateurs (MCI) émet une alarme vers l'administrateur principal (AD), ladite alarme étant perçue par l'administrateur principal comme étant émise par l'équipement dont l'instanciation a été effectuée.

35 14. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce qu'un indicateur est une équation appliquée à des instances d'objets d'une base de gestion d'informations (MIB), les instances étant obtenues par une interrogation des agents (SNMP) fonctionnant sur chacun des équipements du sous-réseau.

40 15. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que le résultat d'un indicateur et/ou une liste des alarmes envoyées peut être stocké dans un fichier archivé sur le disque dur.

16. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que le paramétrage des filtres d'alarmes s'effectue soit par un fichier d'initialisation soit via le protocole snmp

45 17. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que les alarmes à envoyer sont accumulées par le module de confirmation d'alarmes afin de les envoyer groupées, par paquet, à une fréquence donnée.

50 18. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce qu'un modèle de filtre d'alarmes contient une description de l'alarme à reconnaître et un nombre maximal d'occurrence d'alarmes avant lequel une autre alarme est émise vers l'administrateur principal (AD), si ledit nombre maximal d'occurrence d'alarmes est reçu pendant une certaine période.

55 19. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que les différents modules interrogent le noyau (N) pour initialiser leurs paramètres de fonctionnement.

20. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que le noyau (N) gère une base de données contenant toutes les instances de la base de gestion d'informations (MIB), ledit

noyau comportant au moins deux supports (sockets) de communication et une interface commune de gestion de la communication avec les modules.

5 21. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce que les paramètres d'initialisation du module de découverte (MD) comportent la période espaçant deux découvertes, le nombre minimum de systèmes à découvrir et le masque du protocole internet (IP) déterminant l'étendue du réseau à découvrir.

10 22. Système d'administration d'un réseau et d'un système selon la revendication 9, caractérisé en ce qu'un équipement (ET) découvert est classé dans un ou plusieurs domaines en fonction de ses réponses aux interrogations effectuées sur chaque ensemble d'instances d'objets de la base de gestion d'informations (MIB) définissant un domaine.

15

20

25

30

35

40

45

50

55

FIG. 1

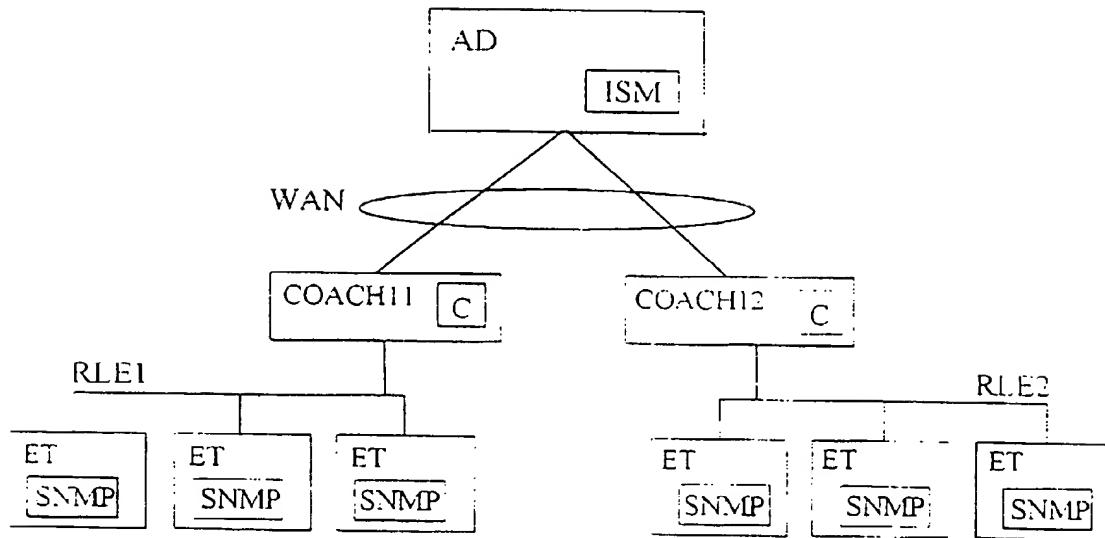


FIG. 4

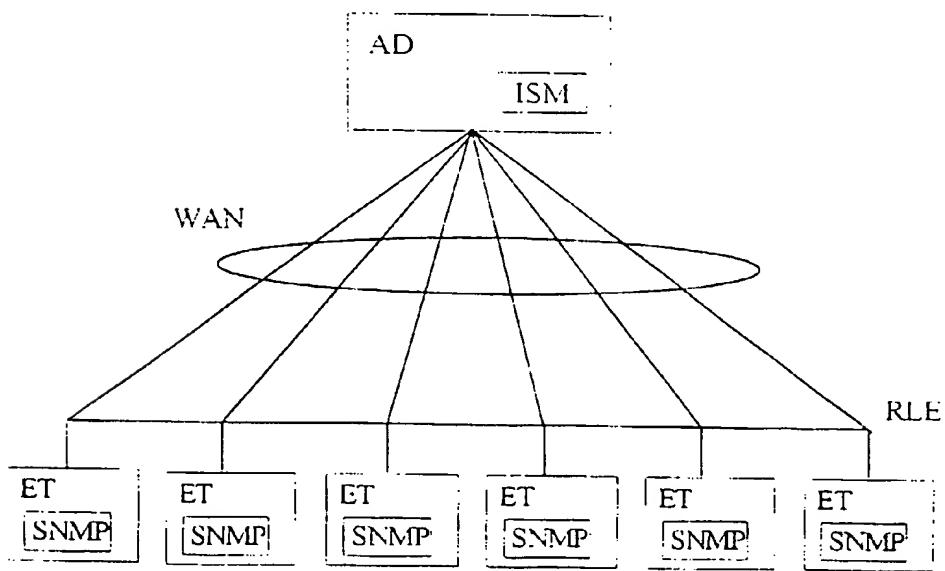


FIG. 2

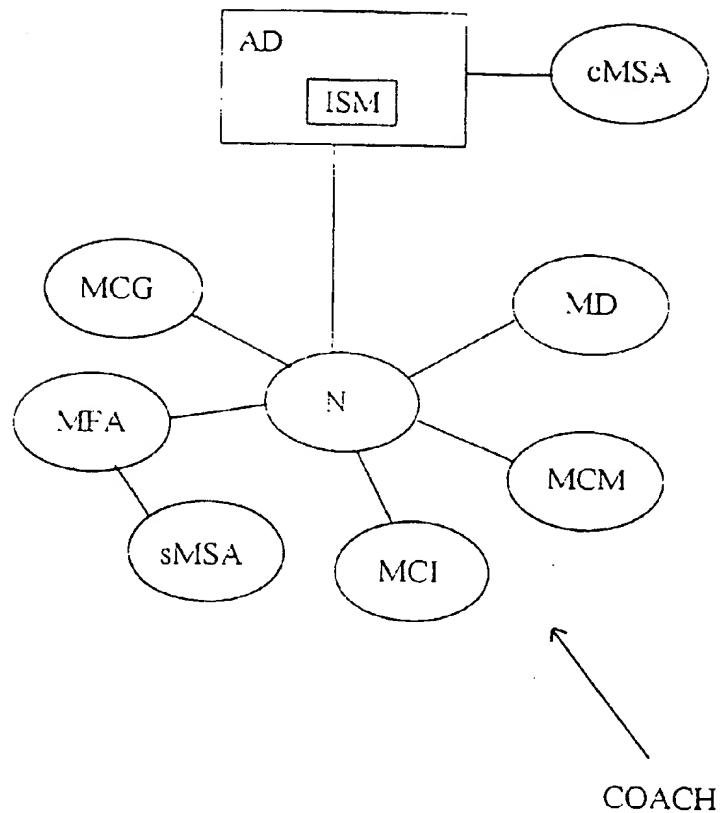
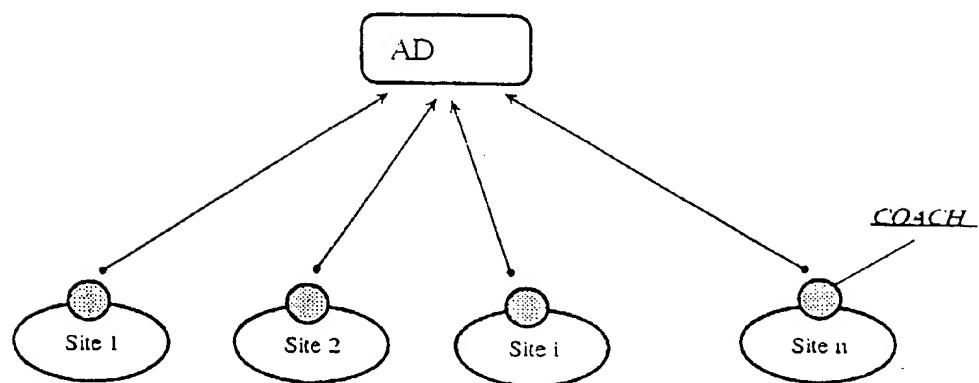


FIG. 3



Office européen  
des brevets

## RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande  
EP 99 40 0808

DOCUMENTS CONSIDERES COMME PERTINENTS			CLASSEMENT DE LA DEMANDE (Int.Cl.6)
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
A	US 5 651 006 A (NAKAZAKI SHINICHI ET AL) 22 juillet 1997 (1997-07-22)	1,11,12, 17	H04L12/24
Y	* abrégé * * colonne 1, ligne 5 - colonne 3, ligne 38 * * colonne 5, ligne 36 - colonne 7, ligne 47 * * colonne 8, ligne 64 - colonne 9, ligne 38 * * colonne 11, ligne 26-47 * * colonne 12, ligne 31 - colonne 13, ligne 26 * * colonne 13, ligne 63 - colonne 14, ligne 19 * * colonne 14, ligne 44 - colonne 15, ligne 8 *	9,10	
Y	PATENT ABSTRACTS OF JAPAN vol. 097, no. 008, 29 août 1997 (1997-08-29) & JP 09 101929 A (HITACHI LTD;HITACHI PROCESS COMPUT ENG INC), 15 avril 1997 (1997-04-15) * abrégé *	9,10	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
	---	---	H04L
		-/-	
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche	Date d'achèvement de la recherche	Examinateur	
LA HAYE	26 juillet 1999	Lievens, K	
CATÉGORIE DES DOCUMENTS CITES			
X : particulièrement pertinent à lui seul	T : théorie ou principe à la base de l'invention		
Y : particulièrement pertinent en comparaison avec un autre document de la même catégorie	E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date		
A : antécédent technique	D : cité dans la demande		
O : divulgation non-écrite	I : cité pour d'autres raisons		
P : document intercalaire	& : membre de la même famille, document correspondant		



Office européen  
des brevets

## RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande  
EP 99 40 0808

DOCUMENTS CONSIDERES COMME PERTINENTS			CLASSEMENT DE LA DEMANDE (Int.Cl.6)
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	
A	<p>SIEGL M R ET AL: "HIERARCHICAL NETWORK MANAGEMENT: A CONCEPT AND ITS PROTOTYPE IN SNMPV2" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 28, no. 4, 1 février 1996 (1996-02-01), pages 441-452, XP000553071 * abrégé * * page 441, colonne de droite, ligne 10 - page 444, colonne de gauche, ligne 2 * * page 444, colonne de droite, ligne 14 - page 445, colonne de droite, ligne 3 * * page 446, colonne de gauche, ligne 16 - colonne de droite, ligne 41 *</p> <p>-----</p> <p>EP 0 777 357 A (NCR INT INC) 4 juin 1997 (1997-06-04) * abrégé * * colonne 2, ligne 13-52 *</p> <p>-----</p>	1,9,11, 13-15	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
A		1,9	
<p>Le présent rapport a été établi pour toutes les revendications</p>			
Lieu de la recherche	Date d'achèvement de la recherche	Examinateur	
LA HAYE	26 juillet 1999	Lievens, K	
CATÉGORIE DES DOCUMENTS CITÉS		<p>T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons</p> <p>&amp; : membre de la même famille, document correspondant</p>	
<p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : améne-plan technologique O : divulgation non-écrite P : document intercalaire</p>			

**ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE  
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.**

EP 99 40 0808

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.

Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du  
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

26-07-1999

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5651006	A	22-07-1997	JP	7334445 A	22-12-1995
JP 09101929	A	15-04-1997	AUCUN		
EP 0777357	A	04-06-1997	US JP	5710885 A 9186688 A	20-01-1998 15-07-1997

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82